|  |
| --- |
| 3GPP TR 33.886 V0.4.0 (2023-02) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on enhanced security for Network Slicing Phase 3;(Release 18) |
|   |
|  | 3GPP-logo_web |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 3

1 Scope 5

2 References 5

3 Definitions of terms, symbols and abbreviations 5

3.1 Terms 5

3.2 Symbols 5

3.3 Abbreviations 6

4 Key issues 6

4.1 Key Issue #1: providing VPLMN slice information to roaming UE 6

4.1.1 Key issue details 6

4.1.2 Security threats 6

4.1.3 Potential security requirements 6

4.2 Key Issue #2: temporary slice authorization and slice service area authorization 6

4.2.1 Key issue details 6

4.2.2 Security threats 7

4.2.3 Potential security requirements 7

4.3 Key Issue #3: network slice admission control (NSAC) 7

4.3.1 Key issue details 7

4.3.2 Security threats 8

4.3.3 Potential security requirements 8

5 Solutions 8

5.1 Solution #1: Verification by Primary NSACF 8

5.1.1 Introduction 8

5.1.2 Solution details 8

5.1.3 Evaluation 9

5.2 Solution #2: Protect NSAC procedure in multiple NSACFs deployment scenario 9

5.2.1 Introduction 9

5.2.2 Solution details 10

5.2.3 Evaluation 11

5.Y Solution #Y: <Solution Name> 12

5.Y.1 Introduction 12

5.Y.2 Solution details 12

5.Y.3 Evaluation 12

6 Conclusions 12

6.1 Conclusions to Key Issue #1 12

Annex A (informative): Change history 13

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document identifies key security issues, potential security and privacy requirements and solutions with respect to network slicing Phase 3 work. Specifically,

* Study potential security impact/requirements/solutions (e.g. Steering of Roaming) to support the HPLMN to provide a roaming UE the VPLMN slice information in a secure manner
* Study potential security impact/requirements/solutions to support temporary slices, slice service areas mismatched with TA boundaries, and slices where S-NSSAI not available in some TAs of RA.
* Study potential security impact/requirements/solutions to support secured NSAC procedures in the cases of NSAC for multiple service areas and network controlled UE behaviours.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.261: "Service requirements for next generation new services and markets; Stage 1".

[3] 3GPP TR 23.700-41 “Study on enhancement of network slicing; Phase 3”

[4] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[5] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

#  3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

<ABBREVIATION> <Expansion>

# 4 Key issues

## 4.1 Key Issue #1: providing VPLMN slice information to roaming UE

### 4.1.1 Key issue details

The following requirement for a 5G network is specified in TS 22.261[2] in order to support a roaming UE activating network slice services

*For a roaming UE activating a service/application requiring a network slice not offered by the serving network but available in the area from other network(s), the HPLMN shall be able to provide the UE with prioritization information of the VPLMNs with which the UE may register for the network slice*

A related key issue is also being studied in TR 23.700-41 [3] for possible procedure changes to automatic PLMN selection for a roaming UE requiring a network slice not offered by the serving network but available in the area from other network(s). It is expected that the corresponding security procedure will be affected (e.g. Steering of Roaming in TS33.501 [4]) in order to support the HPLMN to provide a roaming UE the VPLMN slice information.

In this key issue, the following aspects will be studied:

- Would security procedures be impacted? If so which security procedures are impacted in support of HPLMN proving a roaming UE with information about prioritization information of the VPLMNs with which the UE may register for the network slice?

- How to secure the procedures impacted.

### 4.1.2 Security threats

### 4.1.3 Potential security requirements

## 4.2 Key Issue #2: temporary slice authorization and slice service area authorization

### 4.2.1 Key issue details

Temporary slices are being studied in TR23.700-41 [3]. The objective is to support gracefully terminate a network slice and avoid abrupt PDU Session release.

Temporary slices are expected to be made known to UE during configuration or other network slicing procedures impacting Configured NSSAI or Allowed NSSAI.

This Key Issue will study security aspects to support temporary slices.

Another sub-issue is slice service area authorization. The current granularity in terms service area authorization is Registration Area (RA), which covers multiple Tracking Areas (TA). The key issue needs also to investigate any impacts to security procedures enabling a different service area than per TA.

### 4.2.2 Security threats

A UE may get access to the network resources even when a network slice is terminated or the UE may not get access to the network slices if lifetime information is not conveyed to UE properly or not aligned amongst UE, PLMN and DN.

### 4.2.3 Potential security requirements

The 5G system shall secure procedures with respect to temporary slices.

## 4.3 Key Issue #3: network slice admission control (NSAC)

### 4.3.1 Key issue details

The network slice admission control (NSAC) issues were studied in Rel-17. It has been agreed in Rel-18 to enhance NSAC features with the following features:

- improved network control of the UE behaviour

- support deploying multiple NSACF

In both cases, better UE admission control is aimed to match the allocated quota. However, potential issues of Denial of service (DoS) attacks to legitimate UEs when the additional features are added to the access control mechanism. The information of actual UE / PDU session usage by a slice, or misinformation provided by malicious UEs or mischievous NFs may not be reflected based on current solutions. For example, a NSACF in a VPLMN updating the number of registered UEs or PDU sessions independently may not provide trusted information to the home NSACF. Another example is when a UE not using a network slice is still counted against quota usage of S-NSSAIs where it is registered. It is notable that an attacker can use legitimate UEs to launch such attacks.

In the TR23.700-41 [3], the issue of how to support network slice admission control (NSAC) involving multiple service areas is being studied, together with multiple solutions accepted. The general assumption is that multiple NSACFs are required, either centralized or distributed. In a roaming scenario, it is assumed that the NSAC may be controlled by an NSACF in the VPLMN or an NSACF in the HPLMN.

However, in a roaming scenario, the information reported by the NSACF in the VPLMN is not verified when it is reported to the HPLMN, i.e. there is no proper home control and a misinformation provided by VPLMN may have negative impact to the slices in other service areas, either in HPLMN or other VPLMN.

The security control in different serving areas/PLMNs could be different. For example. the security measure in some service areas is not as strict as what in other areas, attack surface in PLMN of one region may be higher than other regions, etc. The compromised/malicious NSACFs (for solution#13 in TR23.700-41 [3]) in some high risky serving areas/networks may trigger DoS or other attacks on the home network, e.g., the compromised/malicious (local/distributed) NSACFs in a risky service area may fake the case that the number of registration UEs/PDU sessions is reaching the maximum number, and send Nnsacf\_NSAC\_NumberUpdate\_Request to the Primary NSACF for new quota. The Primary NSACF may allocate more quota to the NSACF in compromised serving area/network while decrease the quota of other “lower load” area. Finally, the service of other serving areas/networks could be impacted as the global maximum number may be exhausted by the compromised/malicious NSACFs. As the attack complexity is relatively low while the availability impact could be high, the risk on the system could be high.

In 5G network, network functions in serving network are not always trusted by HPLMN, and home control was enhanced in 5G security architecture. For example, linking home control to subsequent procedures during/after primary authentication procedures to prevent certain types of fraud from serving network (see 6.1.4 of TS 33.501). If AMF/SMF is compromised, only the service of the attacked area would be impacted. In 3GPP protocol point of view, it can hardly damage the HPLMN and impact service of other areas without involving huge number of “legal” UEs due to better home network control for UE access. However, home control for NSAC procedure is not defined in existing specification. In addition, there’s almost no cost/complexity for the compromised/malicious NSACF to launch (D)DoS attack to HPLMN, while it could cause potential wider service impact.

### 4.3.2 Security threats

The malicious/compromised NSACF(s) in specific area(s) of a PLMN with low security protection may continuously send fake message primary NSACF to indicate the number of registration UEs/PDU sessions is reaching the maximum number, that may cause the primary NSACF to re-distribute the quotas of maximum number of registration UEs/PDU sessions to NSACFs in serving areas, finally impact the service of other benign serving areas.

### 4.3.3 Potential security requirements

The 5G System shall provide a means for preventing the quota of maximum of registration UEs/PDU sessions of a network slice being exhausted by malicious/compromised NSACF(s).

# 5 Solutions

Editor’s Note: This clause contains the proposed solutions addressing the identified key issues.

## 5.1 Solution #1: Verification by Primary NSACF

### 5.1.1 Introduction

This solution addresses the key issue #3.

In this solution, it is proposed that the Primary NSACF at HPLMN should verify UE registration information or PDU session information in the requests from the VPLMN NSACF (VPLMN). The proposed solution supports NSAC procedure with security enhancement linking increased home control.

### 5.1.2 Solution details

In a roaming scenario, multiple and hierarchical NSACFs can be deployed over different PLMNs to support NSAC in multiple areas. And the primary NSACF can be deployed in the HPLMN whereas local/distributed NSACFs can be deployed in the VPLMN.

With reference to figure 5.1.2-1, the steps of the solution are described as follows:

1-2) The AMF or SMF triggers the availability check and update (ACU) procedure and sends the update request to vNSACF as described in TS23.502 [5].

3) vNSACF performs the ACU procedure against its local quota.

4) Based on the local configuration, vNSACF may send an update request to the home NSACF (hNSACF) for verfication or availability check and update.

5) The primary NSACF should verify the validity of the informaiton carried in the update request before performing the availability check and update procedure. If the update request carries UE requistrion information or PDU session information for an S-NSSAI, the Primary NSACF can verify through UDM/UDR whether the UE has registered in the vPLMN or whether the UE is a legitimate subscriber of the S-NSSAI. The ACU procedure will proceed after the verfication is successful.

NOTE: the UDM stores authentication results of UEs after authentication as described in TS 33.501[4]. The primary NSACF can distinguish a message is from the local/distributed NSACF in visited network based on the serving network name. The primary NSACF can request to fetch UE authentication results to the UDM in HPLMN.

6) The primay NSACF responses to the vNSACF. It may provide an updated quota if needed.

7) In case quota information is updated, vNSACF should perform ACU again and update its records accordingly.

8) The vNSACF sends the update response as in TS23.502 [5].



**Figure 5.1.2-1 Procedure for Home NSACF verification**

### 5.1.3 Evaluation

Editor’s Note: Further alignment with SA2 work is ffs.

## 5.2 Solution #2: Protect NSAC procedure in multiple NSACFs deployment scenario

### 5.2.1 Introduction

The solution addresses KI#3 network slice admission control (NSAC), in which malicious/compromised NSACF(s) in specific area(s) of a PLMN or in a VPLMN may launch DoS attack towards the Primary NSACF. The solution suggests the primary NSACF to validate the number of UEs or PDU sessions for a S-NSSAI when received the numbers from a NSACF.

When received NSAC number update request from a NSACF in a serving area/VPLMN, based on pre-configured policy the Primary NSACF may cross check with UDM to confirm the number reported by the NSACF is matched to actual number recorded in UDM for a network slice.

If the numbers are not matched, the primary NSACF may stop normal NSAC procedure with the identified NSACF and may send event to management system.

### 5.2.2 Solution details



**Figure 5.2.2-1 workflow to validate number reported by NSACF**

**Precondition**:

* Policies, which related to whether trigger cross check with UDM after received number update request from a NSACF, are pre-configured in a primary NSACF. The policies may be defined according to threat surface, security control and security posture of the VPLMN or specific serving area the NSACF located, or other criteria.
* Assume S-NSSAI information of registered UEs/PDU sessions is available in UDM.

**Procedure**:

0a. After received UE registration request and completed primary authentication and authorization for the UE, the AMF sends Nudm\_UECM\_Registration request to UDM. Once Nudm\_UECM\_Registration is completed and AMF decides on allowed slice, the AMF sends registration update message or Ack message to UDM to inform about the allowed slices list. The S-NSSAI in this list is the HPLMN mapping of the S-NSSAI in allowed NSSAI of the registration.

0b. After creating PDU session for a UE on a slice, the SMF sends Nudm\_UECM\_Registration request to UDM to register the PDU session with parameters including a S-NSSAI.

1. A NSACF in a VPLMN or specific serving area sends Nnsacf\_NSAC\_NumberOfUEsUpdate\_Request or Nnsacf\_NSAC\_NumberOfPDUsUpdate\_Request to the Primary NSACF. That implies the local maximum or upper threshold number of UEs/PDUs is reached.

2. The primary NSACF check the local policies pre-configured as described in precondition. If cross check with UDM is not needed according to the policies, the primary NSACF goto step 10a directly to perform NSAC for the S-NSSAI and update quota for the NSACF if needed.

3. If cross check with UDM is needed according to the policies, the primary NSACF either scans all possible UDMs of the HPLMN or probably discover UDMs based on pre-configured rules.

4. The primary NSACF sends request to each UDM to get number of registered UEs/PDU sessions in specific VPLMNs or AMFs/SMFs for the S-NSSAI.

5. The UDM generates report for number of registered UEs /number of PDU sessions in a VPLMN/AMF/SMF List for the S-NSSAI.

6. The UDM returns the report to the primary NSACF.

7. The primary NSACF consolidates the numbers collected from all impacted UDMs, and gets the total number of registered UEs/PDU sessions in specific VPLMN/serving area for the S-NSSAI.

8. The primary NSACF compares the total number of registered UEs/PDU sessions based on UDM reports and the maximum number in the Nnsacf\_NSAC\_NumberOfUEsUpdate\_Request (or may be stored locally in primary NSACF).

9a. If the two numbers are matched or deviation is not crossing the configured threshold, the primary NSACF performs NSAC for the S-NSSAI and update quota for the NSACF if needed.

9b. If the two numbers don't match or deviation is crossing the configured threshold, the primary NSACF stop NSAC procedure with the potential malicious NSACF, and may adjust the quota for the NSACF, and report the anomaly to OAM.

10. The primary NSACF sends update response to the NSACF, with success or failure.

### 5.2.3 Evaluation

Editor’s Note: Further alignment with SA2 work is may be needed.

## 5.Y Solution #Y: <Solution Name>

### 5.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 5.Y.2 Solution details

### 5.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

# 6 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

## 6.1 Conclusions to Key Issue #1

Existing SoR mechanism defined in TS 33.501[4] is used for protecting the enhanced slice-aware SoR information, which includes preferred PLMNs for specific S-NSSAIs in the UE subscription

When calculating SoR-MAC-IAUSF, the parameter P2 shall include the slice-aware SoR information.

NOTE: Whether normative work is needed to update the parameter P2 is subject to the work in stage 3.

Annex A (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-06 | SA3#107e AdHoc | S3-221372 |  |  |  | Skeleton of TR33.886 | 0.0.0 |
| 2022-06 | SA3#107e AdHoc | S3-221632 |  |  |  | Incorporating S3-221628, S3-221629, S3-221630, S3-221631 | 0.1.0 |
| 2022-10 | SA3#108e AdHoc | S3-222979 |  |  |  | Incorporating S3-221978 | 0.2.0 |
| 2023-01 | SA3#109e AdHoc | S3-230465 |  |  |  | Incorporating S3-230251 | 0.3.0 |
| 2023-02 | SA3#110 | S3-231619 |  |  |  | Incorporating S3-231507, S3-231508, S3-231509 | 0.4.0 |